İÇİNDEKİLER

1 EXPLOIT NEDİR? 1

2 EXPLOIT'LERİN ÇEŞİTLERİ NELERDİR? 3

Remote Exploits 3

Local Exploits 4

0 (Zero) Day Exploits 7

3 METASPLOIT NEDİR? 9

4 METASPLOIT KURULUMU VE GÜNCELLEME 11

Linux İçin Kurulum 11

Windows İçin Kurulum 24

5 GENEL KOMUT VE KAVRAMLAR 31

Exploit Seçme 31

Payload Seçme ve Exploit'e uygun Payload'ların Listelenmesi 32

Parametreleri Tanıma 33

Açık Kontrol Etme 35

Exploit'in Uygulanması 36

Exploit Arama 37

Araçlar Hakkında Bilgi Edinme 39

6 AUXILIARY NEDİR? 41

Auxiliary Modüllerine Genel Bakış 41

Scanner 43

Admin 47

Fuzzers 54

Dos 56

Gather 60

Brute Force 66

SSH Brute Force 66
Password Sniffing 69

7 MSFPAYLOAD 71
MsfPayload Nedir? 71
Payload'ın Oluşturulması 71
Merak Edilenler 86
Remote Payload Oluşturma 88

8 MSFENCODE 91
Msfencode Nedir? 91
Encoder'lerin Listelenmesi ve Tanınması 91
Msfpayload ile Birlikte Kullanımı 93

9 MSFCLI 99
Msfcli Nedir? 99
Hızlı İşlem Yapısı 99

10 MSFVENOM 105

11 İLERİ SEVİYE PAYLOAD & CLIENT SIDE EXPLOIT 109
Meterpreter 109
Meterpreter Üzerinde Bulunan Script'ler 113
Sistemin Command Oturumuna Giriş 115
Otomatik Connect Script Yapımı 116
Adduser 119
File Format Exploit'ler 120

12 EXPLOIT SONRASI İŞLEMLER (POST EXPLOITATION) 125
Dosya İşlemleri 125
Dosya İndirme 125
Dosya Upload 126
Dosya İçeriği Okuma 127

Dosya Silme 127
Ekran Görüntüsü Alma 128
Ses Kaydı Alma 129
Webcam Görüntüsü Alma 130
Irb Command 134
Packet Sniffing 142
Antivirüs ve Fırewall Kapatma 148
Browser'lardan Bilgi Çekme 156
Keylogger 159
İzleri Temizleme 162
Yetki Yükseltme İşlemi 164
Herhangi bir Process'e Bulaşma 169
Sistemde İçerik, Dosya Arama 171
Backdoor'un Kalıcılığını Sağlama Yöntemleri 172
Yüklü Olan Uygulamaların Versiyonlarını Öğrenme 176
Dns Spoffing İşlemi 176
Kullanıcının Aktifliğini Test Etme 179
Kullanıcı Denetimini Kapatma 179
Bazı Donanımların Kontrolünü Sağlama 181
Toplu Script Çalıştırma İşlemi 181
Psexec Pass The Hash 183

13 İLERİ SEVİYE METASPLOIT 187
VNC Connect 187
Linux Backdoor 189
Antivirüs Atlatma Script'leri 190
Php Backdoor 200
Metasploit ile Web Uygulama Testi 203
ShellShock Exploiting 209
Sqlmap With Meterpreter Injection 212

14 NESSUS VULNERABILITY ASSESSMENT 217

Nessus Kurulumu & Aktivasyon 218

İnceleme ve Tanıma 229

Nessus ile Ağ Arası Penetration Test 229

Metasploit ile Nessus Plug-in'lerini Kullanarak Tarama Yapma 243

15 METASPLOIT İLE METASPLOIT LAB. UYGULAMALARI 251

Metasploitable Kurulumu 251

Sistemi Tespit Etme 258

Tespit Edilen Sistemin Açık Port ve Servislerini Tarama 260